AJ

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/831,491	08/08/2001	Teow Hin Ngair	Q64409	5659

7590 01/27/2005

Sughrue Mion Zinn
Macpeak & Seas
2100 Pennsylvania Avenue NW
Washington, DC 20037-3213

EXAMINER
ABYANEH, ALI S

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 01/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Offic Action Summary	**Application N .** 09/831,491	**Applicant(s)** NGAIR, TEOW HIN	
	Examiner Ali S. Abyaneh	**Art Unit** 2133	

-- Th MAILING DATE of this communication appears n the cover sheet with the correspondenc address --

Period f r Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 09 May 2001.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-20 is/are pending in the application.

4a) Of the above claim(s) 10-12 is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-9 and 13-20 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 09 May 2001 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 2/12-16-02.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-9,13-20 are presented for examination. Claims 10-12 are canceled

Information Disclosure Statement PTO-1449

2. The Information Disclosure Statement submitted by applicant on 09/06/2001 and 12/18/2002 has been considered. Please see attached PTO-1449.

Claim Objections

3. Claims 9 and 17 are objected to because of the following informalities:

Regarding claim 9

In claim 9 word "whish" is a typo and should be changed to "which".

Appropriate correction is required.

Regarding claim 17

Claim 17 is objected to because it is dependent on a canceled claim.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Regarding claim 1

The term "token bound output data" in claim 1 is a relative term which renders the claim indefinite. The term " token bound output data " is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree.

(Examiner interprets token bound output data as output data).

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claim 18-20 are rejected under 35 U.S.C. 102(b) as being anticipated by George M. Dolan et al. (US Patent NO.5,604,801).

Regarding Claim 18

Dolan explicitly teaches a token supporting a symmetric key operation to generate a token signature from input data. (column 6, lines 58-67 and column 7, lines 1-9).

Regarding Claim 19 and Claim 20

Dolan explicitly teaches a token (smart card) as claimed in claim 18 wherein the token (smart card) further stores a private key for a digital transaction signature operation. (column 6, lines 57-58).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) patent may not be obtained though the invention is not identically disclose or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over George M. Dolan et al. (US Patent NO.5,604,801) in view of Frank W. Sudia et al.(US Patent NO.6,209,091).

Regarding Claim 1, 8 and 16

Dolan et al. substantially teaches a method (apparatus) of generating a private key signature in respect of user data using a token, the token having stored therein a private key and a symmetric key, said method comprising the steps of providing the user data or a representation thereof as an input to a symmetric key operation supported by the token, (Column 6, lines 58-63) retrieving the output of the symmetric key operation as the token signature, (Column 7, lines 4-6). Dolan does not disclose combining the token signature with the user data to generate the token bound output data and providing the output as an input parameter to a private key signature generation operation, to form a private key signature for the user data; and user data or representation is split into a plurality of block and separate token signature are generated for each block, the token signature being all combined with the user data or representation to generate the token bound out put data. However in an analogous art Sudia substantially teaches a method (apparatus) of combining the token signature with the user data or representation to generate the token bound output data; providing the output data as an input parameter to a private key signature generation operation, to form a private key signature for the user data; and user data or representation is split into a plurality of blocks and separate token signatures are generated for each block, the token signatures being all combined with the user data or representation to generate the token bound output data. (Column 4 lines 45-67 and column 5, lines 1-59). Therefore it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method (apparatus) disclosed by Dolan to include the steps of generating token bound output data and form a private key signature for the user data and split user data into plurality of blocks, generate separate token signatures for each block and combine token signature with user data to generate token bound output data. This would have been obvious because this method of signing would improve security and flexibility by providing a signing system which permits loss or compromise of one or more signing devices while maintaining available un-compromised signing services.

Regarding Claim 3

Dolan et al. explicitly teaches a method which the representation generated using a hash function. (column 6, lines 59-60)

Regarding Claim 4

Dolan et al. substantially teaches a method comprising the step of Generating a session key for each symmetric key operation.(column 7, lines 45-67).

Regarding Claim 5

Doland et al. explicitly teaches a method wherein the session key is generated by modifying a symmetric key stored in the token with a random number. (column 6, lines 45-67).

Regarding Claim 6

Dolan substantially discloses all limitations as applied to claim 4 above but Dolan does not teach a method wherein steps (a) and (b) are conducted recursively and the respective token signatures combined as a single combined token signature. However in an analogous art Sudia substantially teaches a method wherein steps (a) and (b) are conducted recursively and the respective token signatures combined as a single combined token signature. (column 4, lines 46-67 and column 5, lines 1-37).Therefore it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Dolan to conduct the steps (a) and (b) recursively and combine the token signature as a singled combined token signature. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, since the security of the system is enhanced by generating partial signatures and combine all signature as single combined signature.

Regarding claim 7

Dolan substantially discloses all limitations as applied to claim 4 above but Dolan does not disclose the steps of processing the output data to generate a further input related to the output data; applying steps (a) and (b) to the further input to create a session bound output and combining the session bound output with the output. However in an analogous art Sudia substantially teaches the steps of processing the output data to generate a further input related to the output data; applying steps (a) and (b) to the further input to create a session bound output and combining the session bound output with the output. (Column 4 lines 45-67 and column 5, lines 1-59). Therefore it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Dolan to include the steps of generating a further input related to output data, creating session bound output and combining session bound output with a token bound output. This would have been obvious because this method of signing would improve security and flexibility by providing a signing system which multiple signing devices each create, modify, or combine one or more partial signatures, and the result of operations by multiple signing devices produces a single digital signature.

Regarding Claim 14

Dolan explicitly teaches a method wherein the token signature is verified at a secure location at which the symmetric key is stored.(Column 7, lines 4-9).

Regarding claim 15

Dolan explicitly teaches a method as claimed in claim 14

Wherein the location is a secure access module. (Column 6, lines 34-41).

9. Claims 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dolan et al. (US Patent NO. 5,604,801) further in view Frank W. Sudia et al.(US Patent NO.6,209,091) further in view of Vance Bjorn (US Patent NO. 6035398).

Regarding claim 2

Dolan in view of Sudia teach all limitation of the claim as applied to claim 1 above but do not teach representation is a fingerprint of the user data. However, in an analogous art Bjorn discloses a method which representation is a Fingerprint of the user data. (column 4, lines 4-25 and fig 3).Therefore one of ordinary skill in the art at the time the invention was made would have clearly recognized that it is quite advantageous to modify Doland's and Sudia's method to include the representation as a fingerprint of the user data . This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, in order to provide cryptographic key that is easily usable by the user, but not accessible to third party.

10. Claims 9 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dolan et al. (US Patent NO. 5,604,801) further in view Frank W. Sudia et al. (US Patent NO.6,209,091) further in view of Scott A. Vanstone et al. (US Patent NO. 6,490,682).

Regarding Claim 9

Dolan in view of Sudia teach all limitation of the claim as applied to claim 1 above but do not explicitly disclose a method wherein the token signature and private key are output from the token to a computer terminal which uses the private key to perform the private key signature generation operation. However Vanstone substantially teaches a method wherein the token signature and private key are output from the token to a computer terminal which uses the private key to perform the private key signature generation operation. (column 2, lines 23-67 and column 3, lines 1-4).Therefor it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Dolan and Sudia to include the steps of outputting the token signature and private key from token to a computer terminal which uses the private key to perform the private key signature generation operation. This modification would have been obvious because person having ordinary skill in the art would have been motivated to generate a signature key on the terminal in order to verify presented data from token by the terminal.

Regarding claims 13

Dolan in view of Sudia teach all limitation of the claim as applied to claim 1 above but do not explicitly disclose a method of verifying a private key signature generated by comprising the steps of using a signature verification operation to verify the token bound output data and re-generating the token signature using the symmetric key to verify the token. However Vanstone substantially teaches a method of verifying a private key signature generated by comprising the steps of using a signature verification operation to verify the token bound output data and re-generating the token signature using the symmetric key to verify the token.(column 2, lines 52-67 and column 3, lines 1-4).Therefoer it would have been obvious to person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Dolan and Sudia to include the steps of using signature verification operation to verify the private key and re-generating token signature using the symmetric key to verify the token. This modification would have been obvious because person having ordinary skill in the art would have been motivated to verify token out put and regenerate token signature in order to enhance and improve the security.

Ref r nc s Cited, N t Used

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

1. U.S.Patent No.5,943,423

This reference relates to an electronic transaction system which utilizes a smart card or smart token .

2. U.S.Patent No. 5,937,066

This reference relates to a cryptographic key recovery system.

3. U.S.Patent No. 6,185,316

This reference relates to an apparatus, method, and a computer program for self-authentication of an image.

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ali Abyaneh whose telephone number is (571) 272-7961. The examiner can normally be reached on Monday-Friday from (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on (571)272-3819. The fax phone numbers for the organization where this application or proceeding is assigned as (703) 872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from

either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ali Abyaneh
Patent Examiner
Art Unit 2133

Jan 10, 2005

AA

Guy J. Lamarre
Primary Examiner